Navigating Healthcare's Biggest Cybersecurity Challenges in 2018

HIMSS Analytics cybersecurity survey discovers provider concerns around endpoint security, ransomware, emails and phishing, and patient portals

Healthcare providers are a hot target

Cyberattacks on healthcare providers are increasing in frequency and intensity. A recent HIMSS Analytics survey, commissioned by Palo Alto Networks, targeting chief information officers (CIOs), information technology (IT) directors and IT managers at U.S. inpatient healthcare providers, found that two-thirds of survey respondents reported an increase in the frequency of cyberattacks over the past six months (Figure 1).[1]

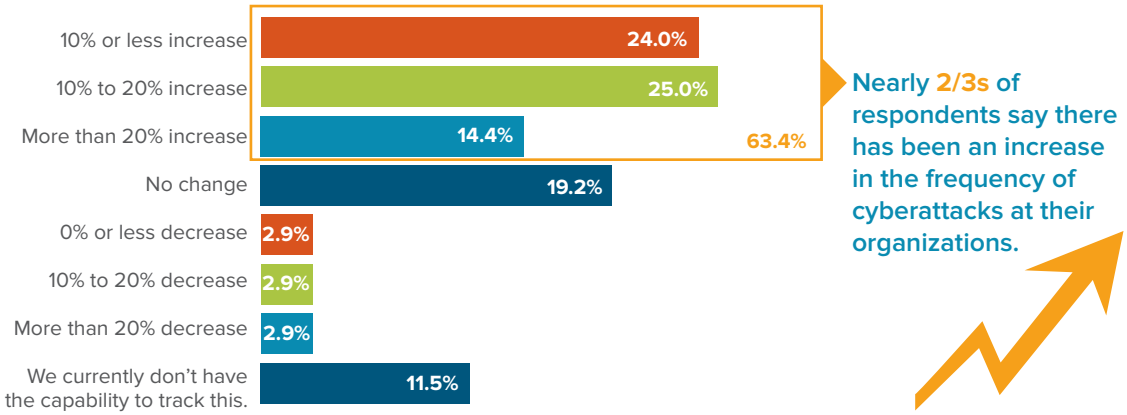
Vast scope of patient data

One of the reasons cyberattackers focus on healthcare is the vast scope of patient data contained within hospital IT networks. Hospital records contain not only protected health information (PHI), but also plenty of other valuable data, from Social Security numbers to credit card information. "There is a wealth of patient information available on a hospital network," said Dwight Hobbs, security engineer at Lancaster General Health/Penn Medicine. "If you can get into the network, you can access that information for a lot of different patients. That makes hospitals a great target for cyberattackers.

Technology heterogeneity

A second reason cyberattackers target hospitals and healthcare organizations is because of the hospital network's technological heterogeneity. Hospitals use countless diverse technologies from a variety of different vendors "and all of those vendors have a different security posture," said Hobbs. "It's difficult for healthcare organizations to maintain a consistent security posture when there are so many variables. It makes it easy for attack-

Figure 1. Cyberattacks in the healthcare environment are increasing (Source: HIMSS Analytics survey).
Over the last six months, how would you describe the change in frequency (if any) of cyberattacks at your organization?



Produced in partnership with HIMSS Media

Produced in partnership with HIMSS Analytics

ers to find a weak spot." A single vulnerability in one device or application can be all an attacker needs to gain access to the entire system.

Cybersecurity not a priority

A third reason cyberattackers prey on the healthcare industry is that quality patient care, not cybersecurity, is the main priority for healthcare organizations. Consequently, cybersecurity has not always been a priority at budget time. "Most healthcare organizations don't have the budget or headcount they need to deal with cybersecurity threats," said Phil Lerner, vice president of technology for United Healthcare Group. "Once there is an incident, then the budget tends to open up. But of course, by then it's too late."

What is top of mind for HC?

HIMSS Analytics undertook the survey to discover providers' top-of-mind cybersecurity concerns for 2018.[2] Among their top concerns were security for endpoints and medical devices, ransomware, phishing education and vulnerabilities related to patient portals. Mitigating the risks associated with these challenges will require a focused effort on the part of healthcare providers. "Today's cybersecurity threats can create really dangerous situations for patients," said Matt Mellen, security architect for healthcare at Palo Alto Networks. "You can't separate cybersecurity from patient care anymore."

The importance of security for endpoints and medical devices

Endpoint security is a critical component of a healthcare provider's overall security posture. "All of the PHI in a hospital network is ultimately on an endpoint, whether that endpoint is a server or a workstation," said Mellen. Endpoint security is complex in healthcare organizations because of the number and variety of endpoints that connect to the enterprise network. A typical hospital network comprises hundreds – or even thousands – of endpoints, including smartphones, tablets, laptops and any number of internet-connected medical devices, from imaging machines to infusion pumps.

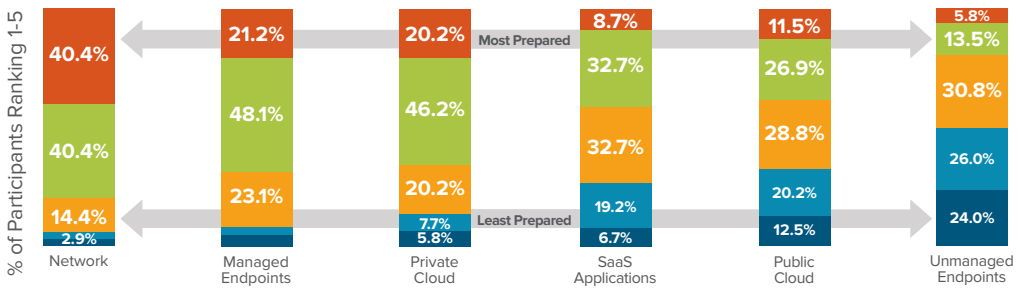
Further complicating the issue is the fact that many of the endpoints in a hospital environment may be managed by the vendor, rather than the hospital itself. "Some vendor-managed devices may be running Windows 95, or another unsupported operating system," he said. "Oftentimes, they don't have any antivirus or endpoint protection installed on them. So they can be very vulnerable devices compared to other devices on a hospital network."

The survey found that healthcare providers feel "least prepared" to deal with unmanaged endpoints, i.e., endpoints not managed by the hospital. Survey respondents ranked unmanaged endpoints as a greater concern than the network itself, managed endpoints, software-as-a-service (SaaS) or the public cloud (Figure 2). Inadequate endpoint protection can be exploited by cyberattackers to deploy malware, such as ransomware, into the hospital environment.

The rise of ransomware

Nearly 90 percent of survey respondents said their organization was targeted with an attempted ransomware attack within the past year (Figure 3). The remaining 10.5 percent of respondents stated they don't currently have technology in place to track the number of ransomware attempts. The rise of ransomware shows how cyberthreats evolve as technology changes. "Ten years ago, ransomware wasn't a concern," said Dylan C. Border, network and security administrator at Fisher-Titus Medical Center. "Back then, it would be more likely you would get a virus in your system that would delete all

Figure 2. Organizations feel most prepared to stop cyberattacks on the network, yet unmanaged endpoints are a concern (Source: HIMSS Analytics survey). Please rate your organization's readiness to stop cyberattacks in the following areas that your data resides: On a scale of 1-5 (1=least-prepared, 5=most prepared)



Notes:
Respondents feel the least prepared in stopping cyberattacks on unmanaged endpoints.
Respondents feel most prepared to stop cyberattacks on the network.
Respondents are more confident in stopping cyberattacks when using a Private Cloud than a Public Cloud, with 28% more individuals ranking it a 4 or 5 on the preparedness scale.

of your data, because that is all the technology allowed for at the time." Today, ransomware is not only possible, it's also extremely lucrative. Instead of stealing medical records and trying to sell them on the black market, threat actors can now hold hospitals hostage and collect their ransom on the spot.

"Your hands are tied if someone has encrypted your data," he said. "You have a tough choice to make. You can either accept the ransom, pay for it, and get your data back. Or, you can be forced to go on without that data. For many organizations, the latter option is not possible, so they can lose tremendous amounts of money." Border anticipates that ransomware will continue to be a problem for healthcare organizations for some time to come. "We won't see the end of ransomware anytime soon," he said. "Ransomware attacks are just going to become more frequent and more sophisticated."

Email protection and phishing prevention

Email offers a popular point of entry for cyberattackers. Email-based cyberattacks account for 94 percent of cyberattacks, according to threat data from over 1,000 global healthcare providers in 2017 on Palo Alto Networks® Next-Generation Security Platform (Figure 4).[3] Why email? "Because it is easy to do and it is universal," said Border. "Email is universal between people, industries and countries. When something is as embedded into our culture and business as email is, that just makes it a gigantic bullseye for cyberattackers to try to exploit."

Email is a particularly challenging area of vulnerability for healthcare organizations because of the human factor. Regardless of how many cybersecurity defenses an organization has in place, at some point, a questionable email is going to arrive in a user's inbox. That is where an organization's user awareness training comes into play. "User awareness training is one of the more bland things we do in information security, but it is really, really important," said Lerner. User awareness training helps the hospital's network users become more sophisticated about what to watch out for in an email, so they aren't caught up in a phishing scheme or worse.

Lerner recommends that user training should be conducted a minimum of quarterly; it should be offered in each user's native language; and it should include an attestation that the user has completed the training and is up-to-date. Organizations can also conduct so-called "Red Team exercises," where agents of the organization try to tempt users into clicking on a phishing-type email. Many companies offer red team exercises so the user gets the experience of actually clicking on a potentially threatening email. This can help organizations determine which users need more training. "Red team exercises should always be treated as a learning opportunity, not as punitive. It shouldn't be a fear-driven event," he said.

In spite of consistent user awareness training, some malicious emails will still make their way into the organization. "People tend to be click-happy," said Lerner. "Even if they are getting consistent user awareness training, some phishing schemes are so sophisticated that unless they are really paying attention, somebody will eventually click on them."

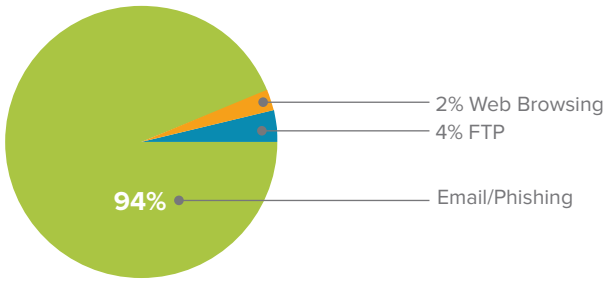
Securing patient portals and patient data

Cybersecurity in a healthcare organization often requires a balancing act between access and security. Patient portals are one of the areas where this balancing act plays out. Forty-eight (48) percent of the respondents in the HIMSS

Figure 3. Ransomware attacks are rampant on healthcare organizations (Source: HIMSS Analytics survey). Approximately how many ATTEMPTED ransomware attacks have been made on your organization in the past year that you are aware of (where a wave of malicious emails counts as one attack)?

> *"Having a security platform is like having a castle with multiple moats around it."*
>
> **Dylan C. Border** | Network and Security Administrator | Fisher-Titus Medical Center

Figure 4. Email-based threats account for 94% of cyberattacks against the healthcare industry in 2017 (Data gathered from Palo Alto Networks AutoFocus™, a cloud-delivered threat intelligence service, based on 590,000 threats observed in over 1,000 healthcare providers globally between 1/1/17 through 6/1/17).



Analytics survey cited patient portal systems as potentially having the biggest impact on the organization's cybersecurity posture in the next 12 months (Figure 5).

The Centers for Medicare and Medicaid Services (CMS) incentivized healthcare providers to facilitate patient engagement through the use of patient portals via the meaningful use program. As a result, most hospitals now offer patient portals.[4] "On the one hand, patient portals are great. You want patients to be able to access their own healthcare information and use it," said Hobbs. "On the other hand, the more ways you open up your system, the more doors you are providing for attackers."

As with email, security around patient portals relies partially on users themselves. Strong password policies, as well as the implementation of two-factor authentication for admin portal access, are two ways to bolster security around patient portals. "In addition to that, network-level deterrents, such as firewalls, can help organizations look for attacks on patient portals and detect them while they are happening so they can be stopped," said Hobbs.

How an integrated security platform provides in-depth protection

No single security device or point product exists that will mitigate all of the cybersecurity risks facing healthcare providers in 2018 and beyond. Endpoint security, ransomware, phishing and the security of patient portals will continue to be areas of concern for the foreseeable future. At the same time, new cybersecurity threats are evolving, which have yet to be identified.

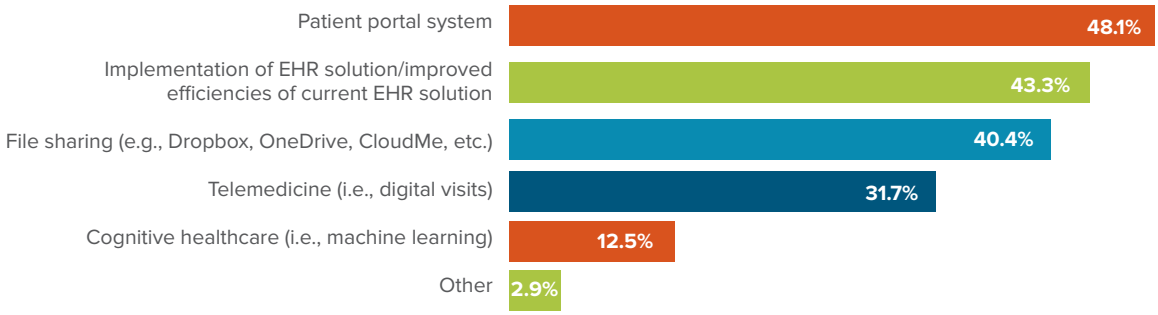
Why the traditional point-product approach is ineffective

Many hospital cybersecurity programs currently rely on a legacy approach to cybersecurity. The legacy approach is characterized by using security products from different security vendors, or security point products, to perform a particular security service (i.e., firewall, network and endpoint-based antivirus, intrusion-detection systems, etc.). While it's important to protect multiple areas of the organization's environment, this approach by itself is no longer sufficient.

Today's threat environment requires a multi-layered approach to cybersecurity based on security enforcement points that natively integrate with each other and share threat information across the entire environment. In other words, if a threat is detected anywhere (e.g., on an endpoint), the platform works to prevent it everywhere (e.g., on the network and in the cloud). The multi-layered approach involving enforcement points that communicate with all other enforcement points is what characterizes a *security platform*. "Having a security platform is like having a castle with multiple moats around it," said Border. "The point is if your enemy gets through one moat, they still have another layer to get through."

> *"If zero trust is deployed properly and efficiently, it can be very effective at stopping ransomware and other types of threats."*
>
> **Dylan C. Border**

Figure 5. Implementation and use of patient portal systems will be a point of interest in the year ahead (Source: HIMSS Analytics survey). What new developments in eHealth will have the greatest impact on you organization's cybersecurity posture in the next 12 months? Select up to 2 answers.



Comprehensive security platform requirements

Healthcare organizations are notorious for having highly heterogeneous computing environments, which means there are many places PHI can be vulnerable to cyberattacks. A robust security platform includes tools to secure each place PHI can go in a healthcare organization – from managed endpoints, like PCs and servers, to vendor-managed endpoints like medical devices, to the network itself and the organization's activities in the cloud. "With a security platform, you have protections beyond what is sitting on your network," said Mellen. "A security platform offers a solution that protects the endpoint on the endpoint, protects the endpoint through the network and protects the endpoint anywhere the data can travel – including the cloud."

An integrated security platform doesn't rely on a single tool or component to stop cyberattackers. Instead, it includes the deployment of multiple tools and strategies across the enterprise. All of these products work together to achieve the same goal: to protect the organization from cyberattacks. Comprehensive security platforms offer hundreds of capabilities. It is impossible to catalog all of those capabilities here. However, the following list includes eight essential capabilities of an effective security platform:

Automated prevention

- ***Coordinate action at all enforcement points through threat intelligence sharing.*** "Native integration of all enforcement points across your security platform allows threat intelligence to pass seamlessly from your network enforcement points to your endpoint enforcement points and vice versa," said Mellen. This ensures that when an anomaly is detected in one part of the security platform, that information is quickly shared across the platform for prevention everywhere.

- ***Automate prevention for real-time protection.*** Most healthcare providers don't have the headcount or skill sets they need to manually respond to the continuing stream of cyberattacks targeting their organization. "A security platform that enables threat intelligence sharing can automate a lot of the security activities that would traditionally be done by a security team," said Mellen.

Next-generation security everywhere PHI exists

- ***Endpoint security products deployed to all endpoints managed by the healthcare organization.*** As noted earlier, a typical hospital includes hundreds – or even thousands – of endpoints. All managed devices within the system should have endpoint protection installed that is effective at preventing malware and exploits – including threats that have never been seen before.

- ***Support the "zero trust" approach to network security.*** In a zero trust network design, there is no default trust for any entity – including internal network traffic. The guideline for zero trust is, "never trust, always verify." "Building a network out this way is extremely difficult, because you have to intimately understand

the traffic patterns in your network, what your databases and applications and web servers are doing," said Border. "If zero trust is deployed properly and efficiently, it can be very effective at stopping ransomware and other types of threats. You need the insight provided by a security platform that has a next-generation firewall at its core to make a zero trust environment work properly."

- ***Reduce risk of unmanaged devices, like medical devices, through next-generation security capabilities.*** Traditional firewalls have limited capabilities and are quickly becoming obsolete. "Next-generation firewalls are much more sophisticated in that they can look at the traffic on a network, identify it to a very granular level and make intelligent decisions based on what that traffic is," said Hobbs. Next-generation firewalls can also mitigate the risks associated with vendor-managed devices, as these devices can be isolated behind the firewall, preventing threats from ever reaching them.

Capabilities to reduce "human factor" risks

- ***Support credential theft prevention to mitigate phishing attacks.*** Credential theft prevention is a feature of very few next-generation firewalls. When a user receives a phishing email, credential theft prevention is a feature that automatically prevents users from sending their user name and password out to a malicious site. This is an effective technology-based method to reduce the "human factor" risks associated with email attacks and phishing.

- ***Integrate with an advanced malware sandboxing service.*** A next-generation firewall can detect concerns such as an email with a potentially malicious file attachment passing from one area of the network to another. The attachment can be automatically sent to a sandboxing service. This provides another way to reduce the "human factor" risks associated with email-based attacks.

Optimized network visibility

- ***Provide real-time or near real-time insight into network traffic.*** A security platform that provides the organization with detailed insight into network traffic is invaluable. A big-picture view of traffic ebb and flow, what applications are being used and the threat level of the users can give information security personnel a better sense of what is taking place at any given moment. "It's important to have real-time insight into the traffic on your network," said Hobbs. "If you can catch cyberattacks as they are occurring, you can work to get ahead of them and head them off before they cause real damage."

The bottom line for healthcare providers is that regardless of the type of threat – whether it be endpoint vulnerabilities, ransomware, phishing or the patient portal – a single line of defense is no longer adequate. "Too many healthcare providers still rely on a collection of legacy, security point products to protect their organizations and their patients from cybersecurity threats. This approach is no longer effective," said Mellen. "However, a multi-layered security platform with natively integrated enforcement points across the network, on the endpoint and in the cloud, provides an in-depth defense to cybersecurity threats that can't be matched by security point products."

HIMSS Analytics Survey Methodology

HIMSS Analytics targeted CIOs, IT directors and IT managers at inpatient U.S. healthcare provider organizations for a web survey that ran from May 4 to June 5, 2017. The survey was completed by 104 respondents from unique institutions. Nearly 33 percent of respondents represented stand-alone hospitals, with 24 percent from hospitals that are part of a delivery system and 17 percent from academic medical centers. Nearly 33 percent of respondents represented provider organizations with 501 or more beds, nearly 31 percent represented organizations with less than 50 beds and 18 percent represented organizations with 101-250 beds.

For the complete HIMSS Analytics 2017 Healthcare IT Cybersecurity Study used in this whitepaper, download it here.

[1] "Healthcare IT Cybersecurity Study", conducted by HIMSS Analytics, commissioned by Palo Alto Networks, October 2017.
[2] Ibid.
[3] Data gathered from Palo Alto Networks AutoFocus™, a cloud-delivered threat intelligence service, based on 590,000 threats observed in over 1,000 healthcare providers globally between 1/1/17 through 6/1/17. quickstats/quickstats.php
[4] The Office of the National Coordinator for Health Information Technology, Health IT Dashboard, "U.S. Hospital Adoption of Patient Engagement Functionalities", retrieved from https://dashboard.healthit.gov/quickstats/quickstats.php
[5] Palo Alto Networks, "Network Segmentation/Zero Trust," n.d. retrieved from https://www.paloaltonetworks.com/solutions/initiatives/network-segmentation

About PaloAlto Networks:

Palo Alto Networks is the next-generation security company maintaining trust in the digital age by helping tens of thousands of organizations and hundreds of healthcare providers worldwide prevent cyber breaches.

Our hospital-grade security platform was built from the ground up for breach prevention, with threat information shared across security functions system-wide, and designed to operate in increasingly mobile, modern healthcare networks. By combining network, cloud and endpoint security with advanced threat intelligence in a natively integrated security platform, we safely enable all applications and deliver highly automated, preventive protection against cyberthreats at all stages in the attack lifecycle without compromising performance.